

***Amendments to the Claims***

The listing of claims will replace all prior versions, and listings of claims in the application.

1. *(currently amended)* A method comprising:

~~receiving computer data from a first computer for transmission to a second computer via a network; and~~

receiving computer data from a first computer at a model of a second computer, the model being maintained and updated to reflect any changes to the second one of the first and second computers;

screening the computer data for at least one virus using the model to produce a screening result; and

~~before communicating the screening result from the model to the computer data to the second computer, wherein said screening comprises creating a model of the second computer, installing a program contained in the computer data on the model, and screening the model for the at least one virus.~~

2. *(currently amended)* The method of Claim 1, further comprising using an wherein the network comprises an IP network for the transmission of the computer data and the screening result.

3. *(original)* The method of Claim 1 further comprising:

if the at least one virus is detected, performing at least one of the following:

(i) inhibiting communication of at least a portion of the computer data to the second computer;

(ii) removing the at least one virus from the computer data prior to transferring the computer data to the second computer;

(iii) communicating a message indicating that the at least one virus was detected to the second computer;

(iv) communicating a message indicating that the at least one virus was detected to the first computer; and

(v) writing data to a database indicating that the at least one virus was detected.

4. (*cancelled*).

5. (*currently amended*) A virus screening device system operative to be connected to a network and operative to screen computer data received from ~~for at least one virus when the computer data is transmitted between~~ a first computer ~~for at least one virus before communicating the computer data to~~ ~~and~~ a second computer, the virus screening device comprising:

~~a third computer on the network that comprises a model of a second one of the first and the second computers computer, the model configured to be maintained and updated to reflect any changes to the second one of the first and second computers and to screen the computer data from a first one of the first and second computers,~~

~~wherein a result of the screening is communicated from the model to the second one of the first and second computers have a program contained in said computer data installed thereon, and wherein said model is further configured to be screened for the at least one virus.~~

6. (*original*) The system of Claim 5, wherein the network comprises an IP network.

7. (*cancelled*).

8. (*currently amended*) The system of Claim 5, ~~further comprising: a third computer communicatively linked to the second computer via~~ ~~wherein the network comprises~~ a local area network, wherein the ~~virus screening device model resides outside~~ the local area network.

9. (*original*) The system of Claim 5, wherein the computer data comprises an electronic mail message.

10. (*original*) The system of Claim 5, wherein the computer data comprises data requested by the second computer from the first computer.

11-13. (*cancelled*).

14. (*currently amended*) The method of Claim 1 [[11]], wherein the ~~network-based virus screening device model~~ resides within a wide area network, and wherein the method further comprises:

receiving across a local area network a request for requested data from the first computer;

sending the request across the wide area network to a the second computer; and  
requesting that the requested data be returned via the model ~~network-based virus screening device~~.

15. (*currently amended*) The method of Claim [[11]] 1, further comprising:  
receiving a request for ~~requested~~ the computer data from the first computer at a modem external to the first computer; and  
initiating communication of the ~~request~~ the computer data from the modem across an IP network to [[a]] the second computer.

16-18. (*cancelled*).

19. (*currently amended*) The method of Claim [[11]] 1, wherein the ~~network-based virus screening device model~~ resides within a wide area network, and wherein the method further comprises:

configuring the ~~network-based virus screening device model~~ to inhibit communication of executables to the first computer; and

configuring an electronic mail system associated with the first computer to route messages addressed to the first computer through the ~~network-based virus screening device model~~.

20. (*currently amended*) The method of Claim [[11]] 1, wherein the first computer is communicatively coupled to a local area network and the ~~network-based virus screening device model~~ resides outside a firewall associated with the local area network, and wherein the method further comprises:

configuring the ~~network-based virus screening device model~~ to inhibit communication of executables to the first computer; and

configuring an electronic mail system associated with the first computer to route messages addressed to the first computer through the ~~network-based virus screening device model~~.

21. (*new*) The method of claim 1, wherein the screening result comprises a version of the computer data.

22. (*new*) The method of claim 21, further comprising using a reduced data version, simplified version, or modified version of the received computer data as the version of the computer data.

23. (*new*) The method of claim 21, further comprising generating a new installation program as the version of the received computer data.

24. (*new*) The method of claim 21, further comprising generating a handshake data packet as the version of the computer program.

25. (*new*) The method of claim 1, wherein the screening comprises screening a portion of the computer data less than all of the computer data for the at least one virus.

26. (*new*) The method of claim 1, further comprising disabling the screening when the computer data is voice data.

27. (*new*) The method of claim 1, further comprising switching between allowing and disallowing the screening based on enabling and disabling signals within the computer data.

28. (*new*) The method of claim 1, wherein the maintaining and updating of the model comprises determining parameters of the second computer, wherein the parameters comprise a version of an operating system, a hardware type, registry information, configuration information, or information from initialization files.

29. (*new*) The method of claim 1, wherein the maintaining and updating of the model comprises requesting information from the second computer, obtaining information from the model if the information was created or altered by the installation program, and requesting information from a pre-existing image of the second computer

30. (*new*) The method of claim, 29, wherein the pre-existing image of the second computer mimics a state of the second computer by maintaining a copy of settings and data stored to the second computer.

31. (*new*) The method of claim 1, wherein the receiving, screening, and communicating of the computer data are performed unidirectionally or bidirectionally between the first and second computers.

32. (*new*) The method of claim 1, wherein at least one of the first computer, the network, or the second computer is subscribed to a service providing the screening.

33. (*new*) The method of claim 1, wherein the model determines from the screening result what is transmitted to the second computer.

34. (*new*) The method of claim 1, wherein the second computer determines from the screening result what is transmitted to the second computer.

35. (*new*) A computer-readable medium containing instructions for controlling at least one processor by a method comprising:

receiving computer data from a first computer at a model of a second computer;  
maintaining and updating the model to reflect any changes to the second computer;

screening the computer data for at least one virus using the model and producing a screening result; and

communicating the screening result from the model to the second computer.

36. (*new*) A system for transmitting computer data between a first computer and a second computer via a network, comprising:

means for receiving the computer data from a first computer, the means for receiving being configured as a model of a second computer and being configured to maintain and update for any changes to the second computer;

means for screening the computer data for at least one virus;

means for producing a screening result therefrom; and

means for communicating the screening result to the second computer.

37. (*new*) A system comprising:

a processor; and

a memory storing instructions that cause the processor to:

. receive computer data from a first computer at a model of a second computer;

maintain and update the model to reflect any changes to the second computer;

screen the computer data for at least one virus using the model and producing a screening result; and

communicate the screening result from the model to the second computer.

38. (*new*) A method, comprising:

causing a intermediary node to receive computer data from a first computer, the intermediary node being a model of a second computer;

causing the intermediary node to be maintained and updated to reflect any changes to the second computer;

causing the intermediary node to screen the computer data for at least one virus using the model and producing a screening result; and

causing the intermediary node to communicate the screening result from to the second computer.

39. (*new*) A method comprising:

maintaining a model of a destination computer;

analyzing data destined for the destination computer to determine whether the data includes a virus; and

providing a screening result to the destination computer.